

T S1/5/1-

1/5/1

DIALOG(R) File 351:Derwent WPI  
(c) 2002 Thomson Derwent. All rts. reserv.

007735513 \*\*Image available\*\*

WPI Acc No: 1989-000625/198901

XRPX Acc No: N89-000535

Data carrier protection against copying - using nest routine to monitor  
given place for changed physical or chemical properties

Patent Assignee: KEESE T (KEES-I)

Inventor: KEESE T

Number of Countries: 001 Number of Patents: 001

Patent Family:

| Patent No  | Kind | Date     | Applicat No | Kind | Date     | Week     |
|------------|------|----------|-------------|------|----------|----------|
| DE 3720233 | A    | 19881222 | DE 3720233  | A    | 19870612 | 198901 B |

Priority Applications (No Type Date): DE 3720233 A 19870612

Patent Details:

| Patent No  | Kind | Lan Pg | Main IPC | Filing Notes |
|------------|------|--------|----------|--------------|
| DE 3720233 | A    | 8      |          |              |

Abstract (Basic): DE 3720233 A

The data carrier (1) during and/or after its mfr. has its properties at at least one place (4) altered w.r.t. the rest of it. The program being protected contains at least one test routine that interrogates the place (4).

Any change in the properties at this place causes the triggering of a program protect routine. The physical and/or chemical properties of the carrier at the place are changed and the place may be tested by a test device. Also described are the data carrier itself (diskette or optical) and its method of mfr.

Title Terms: DATA; CARRY; PROTECT; COPY; NEST; ROUTINE; MONITOR; PLACE; CHANGE; PHYSICAL; CHEMICAL; PROPERTIES

Derwent Class: T01; T03; W04

International Patent Class (Additional): G06F-012/14

File Segment: EPI

?

BEST AVAILABLE COPY



(12) Offenlegungsschrift  
(11) DE 37 20 233 A 1

(51) Int. Cl. 4:  
G 06 F 12/14

(21) Aktenzeichen: P 37 20 233.2  
(22) Anmeldetag: 12. 6. 87  
(43) Offenlegungstag: 22. 12. 88

(71) Anmelder:  
Keese, Thomas, 1000 Berlin, DE  
  
(74) Vertreter:  
Ninnemann, D., Dipl.-Ing., Pat.-Anw., 2800 Bremen

(72) Erfinder:  
gleich Anmelder

Prüfungsantrag gem. § 44 PatG ist gestellt

(54) Kopierschutz für Datenverarbeitungsprogramme

Verfahren zum Schutz eines auf einem magnetischen, optischen, optomagnetischen, elektronischen oder mechanischen Datenträger gespeicherten Programms gegen unberechtigtes Kopieren, wobei der Datenträger (1) während und/oder nach seiner Herstellung mindestens an einer Stelle (4) gegenüber seinen im übrigen Bereich vorgesehenen physikalischen und/oder chemischen Eigenschaften in vorbestimmter Weise verändert wird, daß das zu schützende Programm eine Testroutine aufweist, mit der die betreffende Stelle (4) des Datenträgers (1) abgefragt wird und daß bei einer Abweichung der physikalischen und/oder chemischen Eigenschaften der abgefragten Stelle (4) von den vorgegebenen physikalischen und/oder chemischen Eigenschaften eine Programmschutzroutine ausgelöst wird.

## Patentansprüche

1. Verfahren zum Schutz eines auf einem magnetischen, optischen, optomagnetischen, elektronischen oder mechanischen Datenträger gespeicherten Programms gegen unberechtigtes Kopieren, dadurch gekennzeichnet, daß der Datenträger (1) während und/oder nach seiner Herstellung mindestens an einer Stelle (4) gegenüber seinen im übrigen Bereich vorgesehenen Eigenschaften verändert wird, daß das zu schützende Programm mindestens eine Testroutine aufweist, mit der die betreffende mindestens eine Stelle (4) des Datenträgers (1) abgefragt wird und daß bei einer Abweichung der Eigenschaften der abgefragten Stelle (4) von den vorgegebenen Eigenschaften eine Programschutzroutine ausgelöst wird.

2. Verfahren nach Anspruch 1, dadurch gekennzeichnet, daß die mindestens eine Stelle (4) des Datenträgers (1) so behandelt wird, daß der Datenträger an dieser Stelle seine sonst üblichen physikalischen und/oder chemischen Eigenschaften partiell verändert.

3. Verfahren nach Anspruch 1 oder 2, dadurch gekennzeichnet, daß die in ihren physikalischen und/oder chemischen Eigenschaften gegenüber den sonstigen Eigenschaften des Datenträgers (1) veränderte Stelle (4) von einer Prüfvorrichtung abgefragt und die Adresse der veränderten Stelle (4) bzw. die Adressen der veränderten Stellen (4) in die Testroutinen des zu schützenden Programms eingetragen werden.

4. Verfahren nach einem der vorstehenden Ansprüche, dadurch gekennzeichnet, daß die mindestens eine Stelle (4) des Datenträgers (1) so behandelt wird, daß der Datenträger (1) an dieser Stelle (4) seine physikalischen und/oder chemischen Eigenschaften so verändert, daß nur ein Lesen von an dieser Stelle gespeicherten Informationen, aber kein Beschreiben möglich ist.

5. Verfahren nach einem der vorstehenden Ansprüche, dadurch gekennzeichnet, daß die Änderung der physikalischen und/oder chemischen Eigenschaften des Datenträger (1) an mehreren, auf dem Datenträger (1) verteilt angeordneten Stellen (4) vorgenommen wird.

6. Verfahren nach einem der vorstehenden Ansprüche, dadurch gekennzeichnet, daß der Ort und/oder die Größe und/oder die Änderung der physikalischen und/oder chemischen Eigenschaften des Datenträgers (1) für jeden Datenträger (1) spezifisch ausgebildet werden.

7. Verfahren nach einem der vorstehenden Ansprüche, dadurch gekennzeichnet, daß die Testroutine wahlweise unmittelbar nach der Eingabe des Datenträgers (1) in eine Abtasteinrichtung und/oder im Verlaufe einer oder mehrerer Schreib- und/oder Leseoperationen durchgeführt wird.

8. Verfahren nach einem der vorstehenden Ansprüche, dadurch gekennzeichnet, daß die Testroutine einen Befehl zum Lesen mindestens einer bestimmten Stelle (4), die auf dem Original-Datenträger in spezifischer Weise verändert wurde, und daran anschließend einen Befehl zum Beschreiben der bestimmten Stelle (4) mit einer vorgebbaren oder beliebigen Information abgibt, und daß die Testroutine daran anschließend einen Befehl zum erneuten Lesen der bestimmten Stelle (4) abgibt und bei ei-

ner Änderung des Inhaltes der bestimmten Stelle (4) die Programschutzroutine auslöst.

9. Verfahren nach einem der vorstehenden Ansprüche, dadurch gekennzeichnet, daß die Programschutzroutine aus einer Alarmauslösung und/oder einer anschließenden Selbstlöschung und/oder eines Überschreibens des Programms und/oder einer Unterbrechung weiterer Lese- oder Schreiboperationen besteht.

10. Datenträger zur Durchführung des Verfahrens nach einem der vorstehenden Ansprüche, dadurch gekennzeichnet, daß mindestens eine Stelle (4) auf dem Datenträger (1) in ihren physikalischen und/oder chemischen Eigenschaften gegenüber denen des restlichen Datenträgers (1) abweicht.

11. Datenträger nach Anspruch 10, dadurch gekennzeichnet, daß an mindestens einer vorgegebenen Stelle (4) auf dem Datenträger (1) kein speicherfähiger Raum bzw. keine speicherfähige Schicht vorgesehen ist.

12. Datenträger nach Anspruch 10, dadurch gekennzeichnet, daß an mindestens einer vorgegebenen Stelle (4) auf dem Datenträger (1) ausschließlich lesbare Informationen gespeichert sind.

13. Datenträger nach Anspruch 11 oder 12, dadurch gekennzeichnet, daß an mindestens einer vorgegebenen Stelle (4) auf dem Datenträger (1) kein speicherfähiger Raum bzw. keine speicherfähige Schicht und an mindestens einer weiteren vorgegebenen Stelle (4) auf dem Datenträger (1) eine nur lesbare Information gespeichert ist.

14. Magnetischer Datenträger nach einem der vorstehenden Ansprüche 10 bis 13, dadurch gekennzeichnet, daß an mindestens einer vorgegebenen Stelle (4) auf dem magnetischen Datenträger (1) eine mit einer Information beschriebene magnetisierte Schicht vorgesehen ist, zu deren Überschreiben eine magnetische Feldstärke vorgegebener Größe erforderlich ist.

15. Als Diskette ausgebildeter magnetischer Datenträger nach einem der vorstehenden Ansprüche 10 bis 13, dadurch gekennzeichnet, daß *m*-Bytes der Arbeitsdaten (32) mindestens eines vorbestimmten Sektors (*X*) einer vorbestimmten Spur (*Y*) ausschließlich nur lesbare Daten enthalten oder nicht magnetisierbar sind.

16. Optischer Datenträger nach einem der vorstehenden Ansprüche 10 bis 13 mit einer Laserlichtabtastung, bestehend aus einer kreisförmigen Scheibe mit einem Trägersubstrat, einer Dämpfungsschicht, einer Reflektorschicht, einer dielektrischen Schicht, einer Absorberschicht und einer Schutzschicht, dadurch gekennzeichnet, daß die Absorberschicht (44) und/oder die dielektrische Schicht (43) und/oder die Reflektorschicht (42) an mindestens einer vorgegebenen Stelle (4) so verändert sind, daß wahlweise nur ein Lesen der darin gespeicherten Informationen möglich ist oder keine Informationen speicherbar sind.

17. Vorrichtung zur Herstellung eines Datenträgers mit einem gegen unerlaubtes Kopieren geschützten Programm, gekennzeichnet durch eine Einrichtung zur partiellen Veränderung der physikalischen und/oder chemischen Eigenschaften des Datenträgers (1) an beliebigen Stellen (4) des Datenträgers (1) während oder vor der Übertragung des zu schützenden Programms auf dem Datenträger (1).

18. Vorrichtung nach Anspruch 17, dadurch ge-

kennzeichnet, daß die Einrichtung aus einer Laserdiode besteht.

### Beschreibung

Die Erfindung betrifft ein Verfahren zum Schutz eines auf einem magnetischen, optischen, optomagnetischen, elektronischen oder mechanischen Datenträger gespeicherten Programmes gegen unberechtigtes Kopieren, sowie auf einen Datenträger zur Durchführung des Verfahrens und eine Vorrichtung zur Herstellung eines gegenüber unerlaubtes Kopieren geschützten Datenträgers.

Aus der DE-OS 36 25 176 ist ein Verfahren zur Verhinderung der illegalen Reproduktion einer Aufzeichnung auf einem magnetischen Aufzeichnungsmedium bekannt, bei dem die Position eines Datenbytes in einen spezifizierten Bereich des Aufzeichnungsmediums aus seiner normalen Position verschoben wird, wenn die Daten im Aufzeichnungsmedium aufgezeichnet werden. Dadurch wird ein Lesefehler in derjenigen Position verursacht, in der die Datenbytes verschoben sind, wenn diese Daten im Anschluß an die Aufzeichnung ausgelesen werden, so daß die Wiedergabe der Originalaufzeichnung verhindert wird, da es in dem betreffenden Bereich zu einem Lesefehler kommt. Das bekannte Verschieben von Datenbytes bietet jedoch keine optimale Sicherheit gegen unerlaubtes Kopieren von Programmen, da es innerhalb kurzer Zeit nach Ausarbeitung der neusten Anzahl geschobener Bytes möglich ist, ein spezielles Kopierprogramm zu erstellen, mit dem die Originalaufzeichnung wiedergegeben werden kann.

Aus der DE-OS 35 18 319 ist eine Anordnung zum Schutz von in einer Datenverarbeitungsanlage gespeicherten Programmen gegen unerlaubtes Kopieren bekannt, bei der in der Datenverarbeitungsanlage mindestens ein durch Befehle des Programms adressierbarer und abfragbarer Speicher von den übrigen Speichern der Datenverarbeitungsanlage gesondert angeordnet ist. Der gesonderte Speicher wird an den Daten- und Adressbus der Datenverarbeitungsanlage angeschlossen und vorzugsweise in einem Gehäuse vergossen angeordnet, so daß er nur durch eine Zerstörung des Gehäuses zugänglich ist, wobei beim Zerstören des Gehäuses damit gerechnet werden muß, daß die Codierung des Speichers nicht mehr feststellbar ist. Der gesonderte Speicher wird an bestimmten Stellen im Ablauf des Programms geladen und abgefragt, wobei eine Bedingung für den einwandfreien Ablauf des Programms darin besteht, daß für ein vorgegebenes Datenwort ein zugeordnetes, schaltungsmäßig verschlüsseltes Wort festgestellt wird. Ist dies nicht der Fall, so wird der Ablauf des Programms unter- bzw. abgebrochen. Da sich der Inhalt des gesondert angeordneten Speichers jedoch verhältnismäßig leicht kopieren läßt, kann durch Mitliefern des Inhalts des gesonderten Speichers zusammen mit der Programmkopie der Schutz gegen unerlaubtes Kopieren leicht umgangen werden.

Aus der DE-OS 35 42 128 ist ein Verfahren zum Unterscheiden des Originals eines magnetischen Aufzeichnungsträgers in Form einer Diskette von seinen Duplikaten bekannt, bei dem das Servodatenfeld zur Identifikation einer bestimmten Spur und eines bestimmten Sektors auf der Diskette und das anschließende Datenfeld nacheinander auf die Originaldiskette aufgezeichnet und sowohl das Servodatenfeld als auch das Datenfeld nacheinander bei der Wiedergabe gelesen werden, um damit einen Phasenunterschied an der Schnittstelle

des Datenfeldes wahrzunehmen. Wird ein Duplikat der Originaldiskette hergestellt, so tritt aufgrund der Tatsache, daß die Drehgeschwindigkeit der zum Duplizieren verwendeten Diskette etwas von der Drehgeschwindigkeit der Originaldiskette bei deren Herstellung abweicht, ein Phasenunterschied zwischen dem Anfangspunkt und dem Endpunkt des Datenfeldes der duplizierten Diskette auf, der auch durch eine unregelmäßige Drehung der Diskette auftreten kann. Da es mit den Leseanweisungen für eine normale Diskette nicht möglich ist, das Vorliegen des Phasenunterschiedes an der Schnittstelle wahrzunehmen, kann bei diagnostischen Leseanweisungen oder bei Spurleseanweisungen der Phasenunterschied zwischen dem Datenfeld und dem über dem Zwischenfeld erfaßt und somit festgestellt werden, daß es sich um eine duplizierte Diskette handelt. Dieses bekannte Verfahren eignet sich jedoch nicht zum unmittelbaren Schutz vor einem unerlaubten Kopieren sondern lediglich zur Feststellung eines zuvor erfolgten unerlaubten Kopierens.

Aufgabe der vorliegenden Erfindung ist es, ein Verfahren zum Schutz eines auf einem Datenträger gespeicherten Programmes gegen unberechtigtes Kopieren anzugeben, daß mit für den Datenträger-Hersteller und/oder dem Programmanbieter einfachen Mitteln durchführbar ist und die Anwendung eines auf einen vom Original-Datenträger verschiedenen Datenträger kopierten Programms unmöglich macht bzw. so erschwert, daß ein unerlaubtes Kopieren unrentabel ist. Diese Aufgabe wird durch das kennzeichnende Merkmal des Patentanspruchs 1 gelöst.

Die erfindungsgemäße Lösung ermöglicht es insbesondere dem Programmanbieter, das von ihm angebotene Programm durch eine Modifikation insbesondere der physikalischen und/oder chemischen Eigenschaften des Datenträgers mit einfachsten Mitteln so zu schützen, daß die Herstellung von Raubkopien des so geschützten Programms unmöglich gemacht oder so erschwert wird, daß die Herstellung von Raubkopien unwirtschaftlich wird oder zuviel Zeit beim Herausfinden des Kopierschutzes beansprucht. Dabei kann die Modifikation der physikalischen und/oder chemischen Eigenschaften des Datenträgers an mindestens einer bestimmten oder zufällig gewählten Stelle entweder vom Datenträger-Hersteller vorgenommen und dem Programmanbieter mitgeteilt oder vom Programmanbieter vor dem Herstellen des Originalprogramms durch geeignete Testprogramme herausgefunden werden oder direkt vom Programmanbieter durch eine entsprechende Bearbeitung des Datenträgers durchgeführt werden.

Vorteilhafte Ausgestaltungen der erfindungsgemäßen Lösung sind den Merkmalen der Patentansprüche 2 bis 18 zu entnehmen.

Anhand eines in der Zeichnung dargestellten Ausführungsbeispieles soll der der Erfindung zugrunde liegende Gedanke näher erläutert werden. Es zeigen:

Fig. 1 eine Draufsicht auf eine Diskette zum magnetischen, optischen oder optomagnetischen Speichern von Programminformationen;

Fig. 2 eine vergrößerte Draufsicht auf einen Sektor einer Spur der magnetischen, optischen oder optomagnetischen Diskette gemäß Fig. 1;

Fig. 3 ein vereinfachtes Blockschaltbild einer Datenverarbeitungsanlage mit einer Diskettenstation;

Fig. 4 ein vereinfachtes Flußdiagramm einer Testroutine;

Fig. 5 eine vergrößerte Draufsicht auf einen modifizierten Sektor einer Spur eines optischen Datenträger

und

Fig. 6 einen Querschnitt durch den modifizierten Sektor des optischen Datenträgers gemäß Fig. 5. Die in Fig. 1 dargestellte Draufsicht auf einen magnetischen, optischen oder optomagnetischen Datenträger 1 in Form einer Diskette zeigt in vereinfachter Darstellung mehrere kreisförmige Spuren 2, die in mehrere Sektoren 3 unterteilt sind. Jede Spur 2 weist innerhalb eines Sektors 3 einen Datenvorsatzabschnitt oder Servodataabschnitt 31 auf, in dem die Sektor- und Spurenadresse gespeichert ist sowie einen Datenaufzeichnungsabschnitt 32, in dem Arbeitsdaten eingeschrieben sind oder Daten während eines Aufzeichnungsvorganges einschreibbar sind, wobei der Datenaufzeichnungsabschnitt 32 den wesentlichen Anteil der Spurlänge innerhalb jedes Sektors 3 beansprucht.

Je nach Ausgestaltung der in Fig. 1 dargestellten Diskette als optischer, magnetischer oder optomagnetischer Datenträger sind die Daten bzw. Bytes in Form bestimmter Magnetisierungen oder als sogenannte "Bits", d.h. physikalische Löcher vorgesehen.

Erfundungsgemäß weist der Datenträger 1 bzw. die Diskette an mindestens einer Stelle 4, nämlich im Sektor X der Spur Y eine vorzugsweise in ihren physikalischen und/oder chemischen Eigenschaften gegenüber den sonstigen Datenträgereigenschaften veränderte Stelle 4 auf. Diese während oder nach der Produktion des Datenträgers 1 eingebrachte Stelle 4 kann hinsichtlich ihrer Position und/oder ihrer Größe und/oder ihrer spezifischen Eigenschaft für jedes Exemplar dieses Datenträgers 1 individuell ausgebildet sein. Sie kann beispielsweise bei einem magnetischen Datenträger durch ein nicht beschreibbares, weil nicht magnetisierbares "Loch" in der Magnetschicht oder als eine mit einer Mindestfeldstärke geändert werden kann, so daß bei einem Übertragen dieser Information auf einen Kopie-Datenträger ein Überschreiben dieser Stelle mit einem üblichen Lese/Schreibkopf bzw. Magnetkopf möglich ist, während dies bei dem Original-Datenträger infolge der erforderlichen erhöhten Feldstärke nicht möglich ist.

In Fig. 1 ist lediglich aus Gründen der vereinfachten Darstellung nur eine einzige Stelle 4 mit veränderten physikalischen und/oder chemischen Eigenschaften des Datenträgers 1 dargestellt; selbstverständlich kann auch eine Vielzahl derartiger Stellen 4 vorgesehen werden. Die spezifischen Eigenschaften des Datenträgers 1 müssen dem Software- bzw. Programmanbieter entweder vom Datenträger-Hersteller mitgeteilt werden oder er muß sich die Kenntnis der spezifischen Eigenschaften des Datenträgers 1 durch ein geeignetes Testprogramm selbst beschaffen, so daß er bei der Übertragung seines Programms auf den Original-Datenträger weiß, an welchen Stellen 4, die durch entsprechende Sektor- und Spurenadressen gekennzeichnet sind, geänderte physikalische und/oder chemische Eigenschaften des Datenträgers 1 vorliegen.

Die Veränderung einzelner Stellen 4 des Datenträgers 1 kann auch zufällig erfolgen, d.h. durch Herstellungsungenauigkeiten bzw. -fehler hervorgerufen werden. Daran anschließend ist vom Datenträger-Hersteller oder vom Programmanbieter die Platte zu überprüfen und die Adresse der fehlerhaften Stellen festzustellen. Diese Adressen werden dann als "Fehlerstellen" in vorzugsweise mehreren Testroutinen eingetragen, so daß bei der Abwicklung des Kopierschutzprogrammes die betreffenden Adressen der "Fehlerstellen" abgefragt

werden können.

Eine weitere Möglichkeit besteht darin, nach der Herstellung des Datenträgers in einer geeigneten Vorrichtung künstlich Fehlerstellen zu produzieren, indem beispielsweise mittels einer Laserdiode der Datenträger 1 in seinen physikalischen Eigenschaften so beeinflußt wird, daß er beispielsweise seine Speicherfähigkeit verliert.

In Fig. 2 ist eine vergrößerte Draufsicht auf den Sektor X der Spur Y gemäß Fig. 1 dargestellt und verdeutlicht den Aufbau eines Sektors mit entsprechend veränderten physikalischen und/oder chemischen Eigenschaften des Datenträgers 1 an dieser Stelle zum Schutz des auf dem Datenträger 1 gespeicherten Programms gegenüber unerlaubtem Kopieren.

Der Sektor X der Spur Y weist bei einer in Pfeilrichtung verlaufenden Bewegung der routierenden Diskette am Anfang einen Synchronisationimpuls 30 auf, an den sich die Servodata 31 mit der Sektor- und Spuradresse sowie Hilfssignale zum Ausrichten des Abtastkopfes auf die betreffende Spur anschließen. An den Servodataabschnitt 31 schließt sich ein Arbeitsdatenabschnitt 32 an, der normalerweise ausschließlich mit Programm-Bytes beschrieben ist oder zum Einschreiben von Daten dient. Im vorliegenden Fall enthält der Arbeitsdatenabschnitt 32 jedoch einen m-Bytes-Abschnitt, der nur ein Lesen der darin gespeicherten Informationen ermöglicht, während der restliche Arbeitsdatenabschnitt 32 mit n-Bytes sowohl zum Lesen als auch zum Schreiben verwendet werden kann. Abweichend hiervon kann der Arbeitsdatenabschnitt 32 mit mehreren Lese/Schreib-Abschnitten und mehreren nur zu lesenden Abschnitten versehen sein. Alternativ hierzu ist es auch möglich, die m-Bytes-Abschnitte, die die Stellen 4 mit veränderten physikalischen und/oder chemischen Eigenschaften bilden, auch als völlig inaktive Abschnitte auszubilden, so daß an dieser Stelle Informationen weder eingeschrieben noch herausgelesen werden können. Dies kann beispielsweise durch Herausbrennen der Magnetschicht bei einem magnetischen Datenträger mittels eines Laserstrahls oder durch eine geeignete Veränderung der optischen Informationsträgerschicht eines optischen Datenträgers erfolgen.

In Fig. 3 ist ein vereinfachtes Blockschaltbild eines Mikrocomputersystems mit einer Diskettenstation dargestellt. Das Mikrocomputersystem umfaßt einen Mikrocomputer 5, der über eine Takteleitung mit einem Taktgenerator 6 und über einen Adreßbus einen Speicher 7 für ein Anwenderprogramm, einen Datenspeicher 8 und Eingabe/Ausgabe-Bausteine 9 adressiert und wechselseitig über einen Datenbus mit dem Speicher 7 für das Anwenderprogramm, den Datenspeicher 8 und die Eingabe/Ausgabe-Bausteine 9 verbunden ist. Zusätzlich ist der Mikroprozessor 5 über Steuersignalleitungen mit den Speichern 7, 8 und den Eingabe-/Ausgabe-Baustein 9 wechselseitig verbunden.

Die Eingabe/Ausgabe-Bausteine 9 sind über einen Datenbus mit einem Magnetkopf 12 verbunden, von dem sie Programmdaten aufnehmen, die auf einem entsprechenden Datenträger in Form einer Diskette 1 gespeichert sind. Gesteuert wird die Bewegung des Magnetkopfes 12 von einem Linearmotor 11, der wiederum Steuersignale von dem Eingabe/Ausgabe-Baustein 9 empfängt.

Die Diskette 1 ist auf einer Antriebswelle 14 gelagert, die von einem Diskettenmotor 13 angetrieben wird. Der Magnetkopf 12 kann selbstverständlich auch als thermischer, optischer oder elektronischer Abtastkopf ausge-

bildet sein.

Nachstehend soll die Funktionsweise des erfindungsgemäßen Verfahrens und des Datenträgers zur Durchführung des Verfahrens anhand der vorstehend beschriebenen Figuren und des in Fig. 4 dargestellten Flußdiagramms näher erläutert werden.

Eine mit mindestens einer "Fehlstelle" 4 versehene optische, magnetische, optomagnetische, mechanische oder elektronische Datenträgerplatte 1 wird vom Laden des Speichers für das Anwenderprogramm 7 in die Diskettenstation 10 gemäß Fig. 3 eingefügt und vom Tastkopf 12 und der Steuerung des Linearmotors abgetastet. Während des Ladens des Inhalts der Datenträgerdiskette 1 in den Speicher für das Anwenderprogramm 7 oder nach dem vollständigen Laden des Inhalts in den Speicher für das Anwenderprogramm 7 wird eine Testroutine eingeleitet, die darin besteht, daß in der Testroutine ein Befehl auftritt, die "Fehlstelle" 4, d.h. Spur X und Y zu lesen und den Inhalt beispielsweise im Datenspeicher 8 abzulegen. Daran anschließend wird der Befehl gegeben, die Spur X und Sektor Y mit einer beliebigen Bit-Folge zu schreiben und daran anschließend erneut Spur X und Sektor Y zu lesen und den Inhalt des zweiten Lesevorgangs ebenfalls im Datenspeicher 8 abzulegen.

Bei dem daran anschließenden Vergleich wird festgestellt, ob der Inhalt der Spur X und des Sektors Y durch das Schreiben zwischen den beiden Lesevorgängen geändert wurde. Ist dies nicht der Fall, weil nämlich die Originaldiskette als Datenträger verwendet wurde, und Spur X, Sektor Y nur lesbar und nicht beschreibbar ist, so wird das Programmladen fortgesetzt oder das geladene Anwenderprogramm freigegeben.

Wird jedoch eine Änderung des Inhalts der Spur X, Sektor Y festgestellt, weil eine Diskette mit einer Kopie des Programms verwendet wird, bei der an der betreffenden Stelle 4 keine Änderung der physikalischen oder chemischen Eigenschaften der Diskette vorliegt, und so die Möglichkeit besteht, Spur X, Sektor Y auch zu beschreiben, so wird ein Unterprogramm "Programmschutz" aufgerufen, das beispielsweise unsinnige Befehle von der Diskette 1 in den Speicher für das Anwenderprogramm 7 lädt oder zu einer Löschung des gesamten Programms führt, so daß das Programm "abstürzt".

In den Fig. 5 und 6 ist die Anwendung des erfindungsgemäßen Verfahrens auf einen optoelektronischen Datenspeicher anhand einer Draufsicht auf eine Spur und einen Sektor des optoelektronischen Datenträgers und in Fig. 6 anhand eines Querschnitts durch einen Teil der Spur und des betreffenden Sektors mit der abweichen den physikalischen und/oder chemischen Eigenschaft dargestellt.

Fig. 5 zeigt einen vorformatierten Datenvorsatz 31 für die Servodaten, der in jeder Spur und jedem Sektor der optoelektronischen Diskette vorgesehen ist. Er besteht aus einem Synchronisierbit 310 mit einem relativ großen Wechsel der optischen Reflexion, zwei auf beiden Seiten der Spurmittellinie aufeinanderfolgend vorgesehenen Spurfolge-Bits 311, 312 zum Ausrichten des optischen Abtastkopfes auf die Mittellinie der Spur, drei hintereinander angeordneten Fokussierungsbits zum Fokussieren des auftreffenden Lichtstrahls sowie Spurbits für den Sektor-Adresse-Bit 314 zum Identifizieren der betreffenden Spur und des betreffenden Sektors. Daran schließen sich über eine Länge von  $m$  Bytes mehrere NUR-LESE-Bits 321 an, denen  $n$ -Bytes Lese- und Schreib-Bits 322 des Datenfeldes 32 folgen.

Die physikalische Beeinflussung der betreffenden Stelle zum Schutz des Programms gegen unerlaubtes

Kopieren kann in einer in Fig. 6 dargestellten Weise realisiert werden.

Fig. 6 zeigt einen Querschnitt durch die betreffende Spur im Bereich des Endes des Datenvorsatzes 31 und 5 des Beginns des Datenfeldes 32. Die optoelektronische Speicherplatte besteht aus einem Trägersubstrat 40 aus Aluminium, auf der eine Dämpfungsschicht 41 angeordnet ist. Daran schließt sich eine Reflektorschicht 42 aus Aluminium an, die als hochreflektierende opake Schicht 10 ausgebildet ist. Es folgt eine dielektrische Schicht 43, an 15 die sich eine Absorberschicht 44 aus beispielsweise Tellur anschließt. Die obere Schicht 45 dient als Schutzschicht und besteht beispielsweise aus einem Silikonharz. Der Aufbau und die Funktion einer derartigen optoelektronischen Speicherplatte ist beispielsweise in der EP-A-00 89 119 dargestellt und erläutert.

Die Speicherung von Informationen auf dem in Fig. 6 dargestellten Querschnitt durch den optoelektronischen Datenträger 1 erfolgt durch die in die Absorberschicht 20 44 eingebrachten Bits, wodurch ein auf den Datenträger 1 auftreffender Laserstrahl unterschiedlich reflektiert wird. Durch Vorsehen nicht beschriebener Regionen beispielsweise in der Absorberschicht 44 besteht die Möglichkeit, Daten in Form von Bits auf den Datenträger zu schreiben, während bei Vorhandensein von Bits 25 ein solches Beschreiben der Absorberschicht nicht mehr möglich ist. Auf diese Weise ist es möglich,  $m$ -Bytes NUR-LESE-Bits 321 im Datenfeld 32 vorzusehen, so daß der Datenträger 1 mit dem Originalprogramm an dieser Stelle nicht überschreibbar ist. Wird entsprechend dem Flußdiagramm gemäß Fig. 4 der Befehl zum Überschreiben des Sektors Y der Spur X, d.h. der Stelle 30 4, gegeben, so kann durch anschließendes Lesen des Sektors Y der Spur X festgestellt werden, ob es sich um einen Datenträger 1 mit Originalprogramm handelt oder nicht.

Zur Herstellung von Datenträgern, die mit dem oben beschriebenen Schutz gegen unerlaubtes Kopieren versehen sind, kann vorteilhafter Weise eine Vorrichtung 40 verwendet werden, in die ein entsprechender Datenträger mit einem ungeschützten Programm sowie ein unbeschriebener Datenträger, d.h. ein Datenträger ohne gespeicherte Informationen eingegeben werden. Über einer mit der Vorrichtung verbundene Tastatur werden 45 wahlweise "Fehlstellen" eingegeben oder von einem Fehlerschutzprogramm abgegeben werden. Während der Übertragung des ungeschützten Programms auf den unbeschriebenen Datenträger werden die wahlweise auch von einem Zufallsgenerator abgegebenen "Fehlstellen" auf dem unbeschriebenen Datenträger produziert und gleichzeitig die entsprechenden Adressen der 50 "Fehlstellen" in die verschiedenen Testroutinen einge tragen. Nach der vollständigen Übertragung des un geschützten Programms auf den unbeschriebenen Datenträger erhält man einen das betreffende Programm speichernden Datenträger, der nunmehr gegen unerlaubtes 55 Kopieren geschützt ist. Dabei können die "Fehlstellen" beispielsweise in der zuvor beschriebenen Weise mittels einer Laserdiode produziert werden, die die entsprechenden Stellen 4 so behandelt, daß der Datenträger 1 an diesen Stellen 4 seine Speicherfähigkeit verliert oder 60 in vorbestimmter Weise verändert.

Die vorstehend beschriebenen Ausführungsbeispiele sollen nur das Anwendungsspektrum der erfindungsgemäßen Lösung erläutern. Selbstverständlich sind anstelle der beschriebenen Disketten als Datenträger 1 auch Magnetbandspeicher, elektronische, mechanische oder biologische Speicher in Verbindung mit dem erfin-

dungsgemäßen Verfahren zum Schutz des auf dem be-  
treffenden Datenträger gespeicherten Programms ge-  
gen unerlaubtes Kopieren verwendbar.

5

10

15

20

25

30

35

40

45

50

55

60

65

3720233

Int. Cl. 4:  
Anmeldetag:  
Offenlegungstag:

G 06 F 12/14  
12. Juni 1987  
22. Dezember 1988

FIG. 1

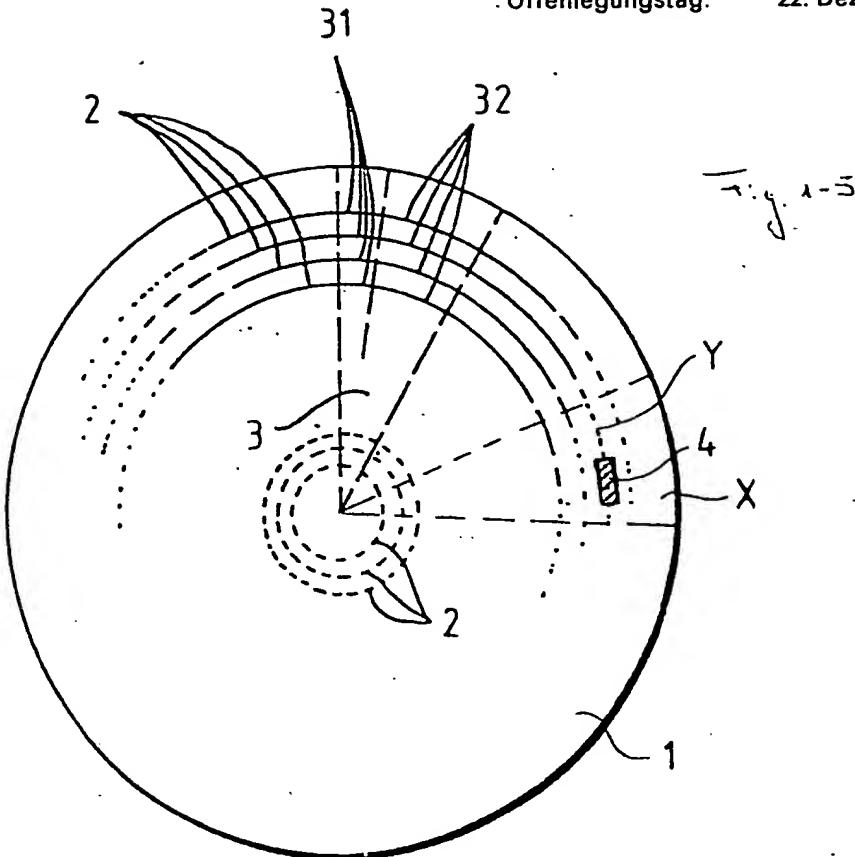
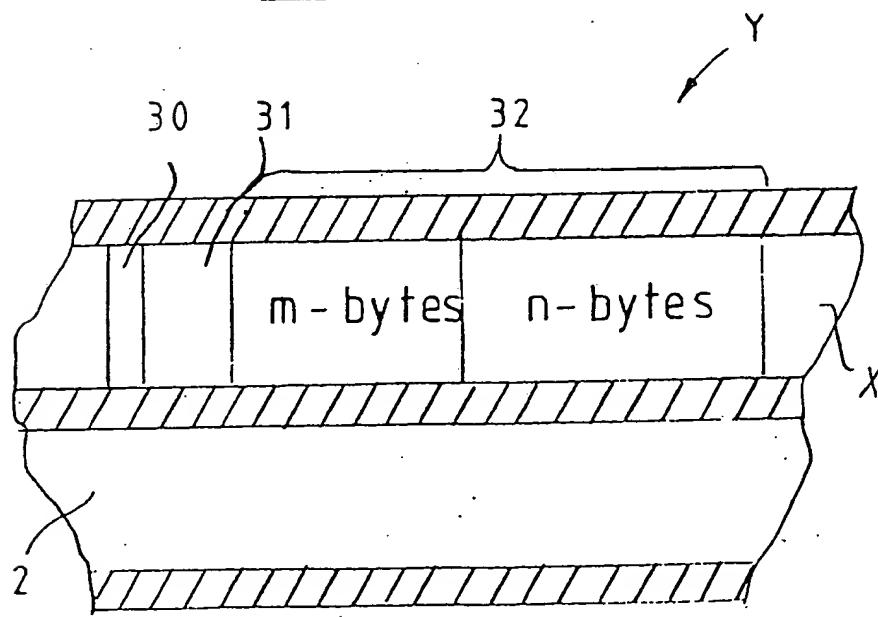


FIG. 2



3720233

xx

FIG. 3

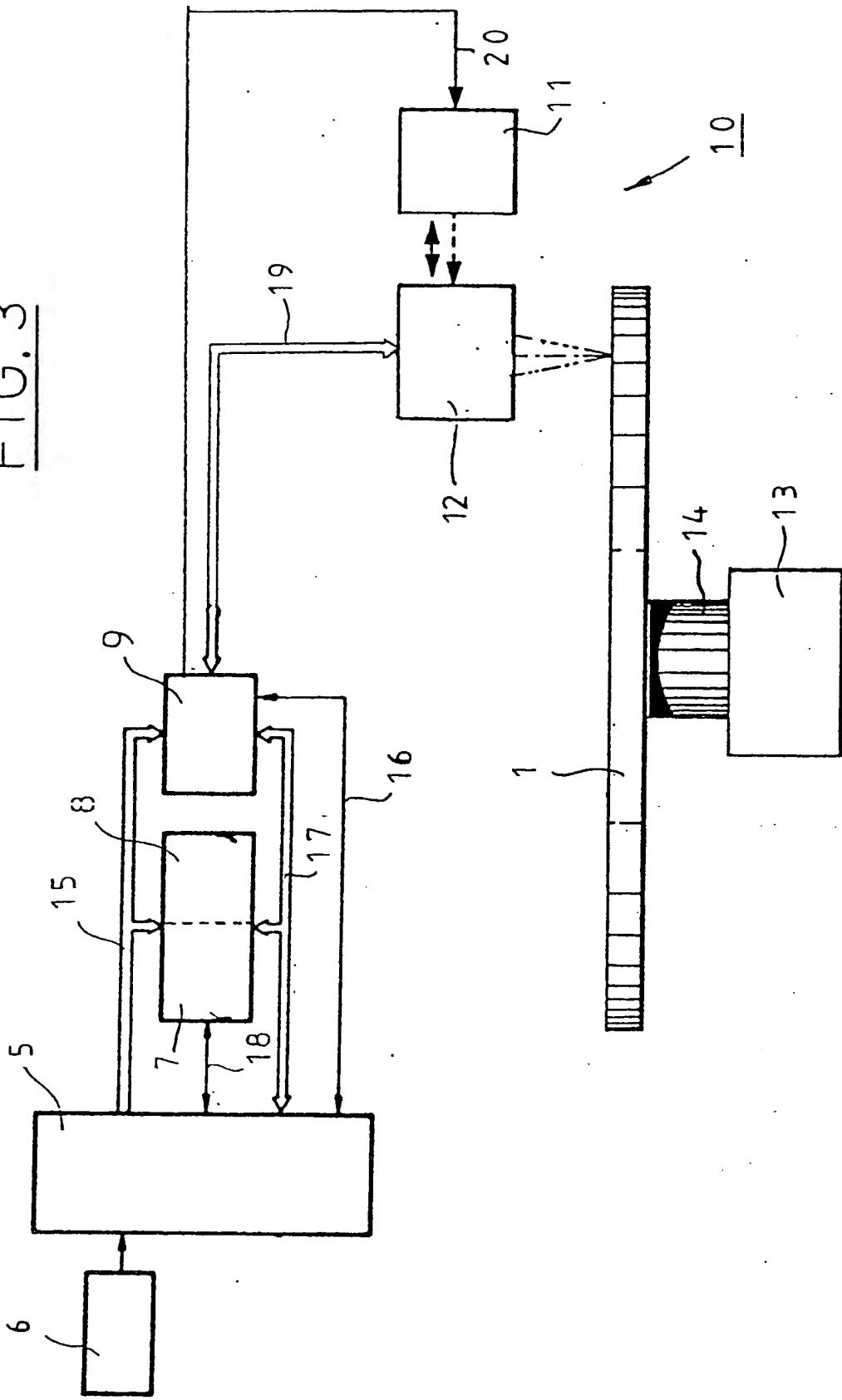
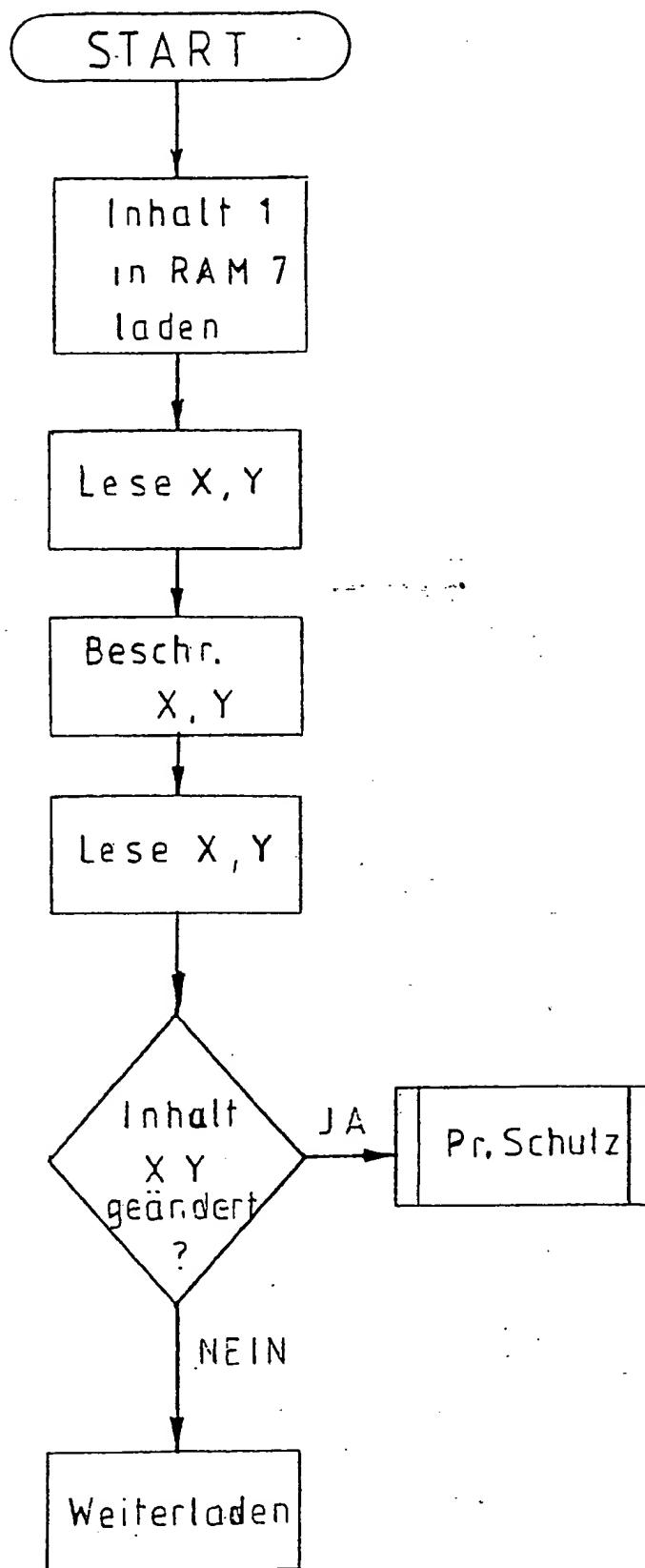


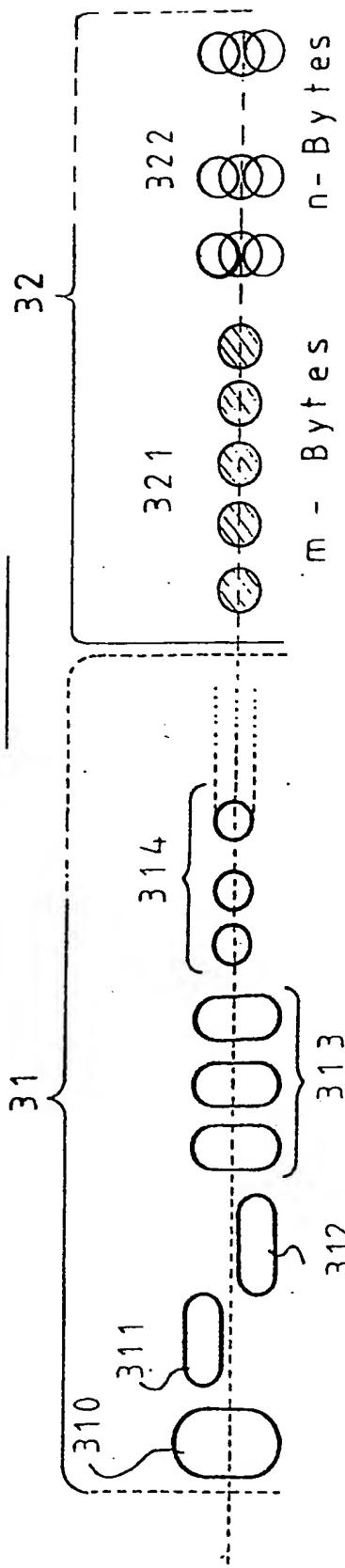
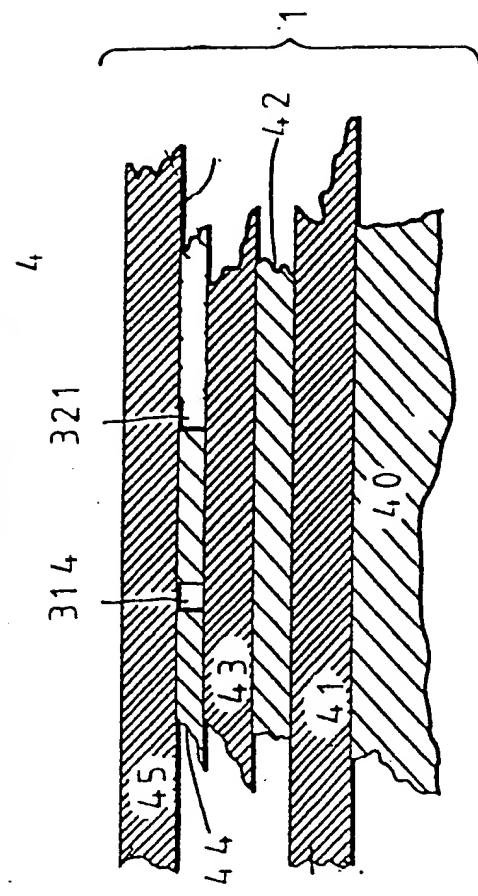
FIG. 4

3720233



24

3720230

FIG. 5FIG. 6

**This Page is Inserted by IFW Indexing and Scanning  
Operations and is not part of the Official Record**

## **BEST AVAILABLE IMAGES**

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- BLACK BORDERS**
- IMAGE CUT OFF AT TOP, BOTTOM OR SIDES**
- FADED TEXT OR DRAWING**
- BLURRED OR ILLEGIBLE TEXT OR DRAWING**
- SKEWED/SLANTED IMAGES**
- COLOR OR BLACK AND WHITE PHOTOGRAPHS**
- GRAY SCALE DOCUMENTS**
- LINES OR MARKS ON ORIGINAL DOCUMENT**
- REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY**
- OTHER:** \_\_\_\_\_

**IMAGES ARE BEST AVAILABLE COPY.**

**As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.**